A mesterséges intelligencia használatának összefoglalása vezetők, döntéshozók számára

A dokumentum tárgya: Az Európai Parlament és a Tanács (EU) 2024/1689 rendelete, azaz az AI Act, valamint a mesterséges intelligencia vállalati használatából eredő jogi, adatvédelmi, információbiztonsági és felelősségi kérdések.

MI-jártasság és vállalati felkészültség

Az AI Act egyik fontos elvárása az úgynevezett MI-jártasság fejlesztése. Ez nem pusztán azt jelenti, hogy a munkavállalók ismerik az MI-eszközök használatát. Azt is jelenti, hogy tisztában vannak:

- az MI lehetőségeivel és korlátaival;
- a használatából eredő kockázatokkal;
- az adatvédelmi és információbiztonsági követelményekkel;
- az MI használatához kapcsolódó jogaikkal és kötelezettségeikkel;
- az MI által előállított eredmények ellenőrzésének szükségességével.

Az MI alkalmazóknak intézkedéseket kell tenniük a saját személyzetük, valamint az MI működtetésében és használatában közreműködő személyek jártasságának fejlesztésére. A szükséges ismeretek szintjét az érintettek szakmai tapasztalatához, képzettségéhez, a rendszer jellegéhez és a felhasználás körülményeihez kell igazítani.

Vezetői szempontból ez azt jelenti, hogy a vállalatnak nem elegendő egyszerűen engedélyeznie az MI használatát: biztosítania kell a megfelelő ismereteket és a szabályozott használati környezetet is.

Az AI Act rendelet célja és alapelve, hogy a rendelet nem váltja ki a GDPR, üzleti titokvédelmi vagy szerzői jogi szabályokat. Részletezi a kockázati besorolást, a tiltott gyakorlatokat, az átláthatósági elvárásokat, az MI jártasság jelentőségét, és rávilágít a felelősség fontosságára. Külön hangsúlyozza, hogy az MI által generált eredményeket ellenőrizni kell, **jogsértő lehet a személyes adatok, üzleti titkok és szerzői jogi védelem alatt álló művek engedély nélküli felhasználása, és jelentős bírságokkal járhat a megfelelés hiánya.**

A tiltott gyakorlatok közé tartozik a manipulatív MI, a sérülékenység kihasználása, a társadalmi pontozás, a profilalapú bűnmegelőzési értékelés, a cél nélküli arckép-adatbázis építése, munkahelyi érzelemfelismerés, bizonyos biometrikus kategorizációk, valamint a valós idejű távoli biometrikus azonosítás nyilvános térben.

Az AI Act által nem rendezett, de kiemelten fontos jogi-és információbiztonsági kérdések

A dokumentum egyik legfontosabb megállapítása, hogy az AI Act nem helyettesíti a hagyományos adatvédelmi, üzletititok-védelmi és szerzői jogi védelmi szabályokat.

ITJUMP KFT.

E-mail: info@itjump.hu

Telefon: (1) 700 1122

Levelezési cím:
1082 Budapest, Corvin köz 4.

itjump.hu
efoki.hu

Az MI használatának kockázatait ezért más jogszabályok alapján is vizsgálni kell. (GDPR, DORA, NIS2)

Személyes adatok védelme
Személyes adat MI-rendszerbe történő bevitele csak megfelelő adatkezelési cél és jogalap mellett történhet. Külső MI-szolgáltatás használatakor tisztázni kell:

- milyen adatkezelési szerepet tölt be a szolgáltató;
- milyen adatmegőrzési szabályokat alkalmaz;
- milyen biztonsági intézkedésekkel védi a bevitt adatokat;
- továbbít-e adatokat harmadik országba;
- felhasználja-e a bevitt adatokat modelljeinek tanítására.

Fontos felhívni a figyelmet arra, hogy az úgynevezett opt-out funkció – amely elvileg megakadályozza a bevitt adatok tanítási célú felhasználását – önmagában nem garantálja a biztonságot.
Következtetés: Amíg az adatkezelési és biztonsági feltételek nem tisztázottak, személyes adatok bevitele külső MI-rendszerbe nem javasolt.

Üzleti titkok és védett ismeretek
Az MI használata során a munkavállalók olyan információkat is megoszthatnak, amelyek üzleti titoknak vagy védett ismeretnek minősülnek.
Ilyenek lehetnek:

- ügyféladatok és üzleti dokumentumok;
- belső stratégiák és üzleti tervek;
- fejlesztési dokumentáció és forráskód;
- műszaki, gazdasági és szervezési know-how;
- üzleti folyamatok és belső elemzések.

Az ilyen adatok MI-rendszerbe történő feltöltése a vállalat számára jelentős versenyhátrányt és jogi kockázatot okozhat. A munkáltató számára javasolt, hogy:

1. határozza meg a munkavégzéshez engedélyezett MI-rendszereket;
2. egyértelműen tiltsa meg a személyes adatok és üzleti titkok MI-rendszerbe történő feltöltését;
3. szabályozza a belső dokumentumok és know-how kezelését.

Az MI által előállított eredmények ellenőrzése és felelősség

Az MI által előállított tartalom helyességének, pontosságának és valóságtartalmának ellenőrzése az alkalmazó felelőssége.
Az MI-rendszerek:

- elavult vagy pontatlan adatokból dolgozhatnak;
- téves következtetéseket vonhatnak le;
- nem létező jogszabályokat és forrásokat állíthatnak elő;
- meggyőző formában közölhetnek valótlan információkat.

A generált tartalom ellenőrzésének elmulasztása komoly következményekkel járhat, különösen akkor, ha a hibás eredményt a munkavégzés során felhasználják. A vállalatnak ezért biztosítania kell, hogy az MI által előállított tartalmakat a felhasználás előtt megfelelő szakmai ellenőrzésnek vessék alá.

Jogkövetkezmények és bírságok

Az AI Act megsértése jelentős pénzügyi következményekkel járhat. A dokumentum az alábbi maximális bírságokat ismerteti:

Jogszabálysértés	Maximális bírság
Tiltott MI-gyakorlat alkalmazása	35 millió EUR vagy a globális éves árbevétel 7%-a
Egyéb meghatározott szolgáltatói és alkalmazói kötelezettségek megsértése	15 millió EUR vagy a globális éves árbevétel 3%-a
Helytelen, hiányos vagy félrevezető információ szolgáltatása	7,5 millió EUR vagy a globális éves árbevétel 1%-a

A vállalkozások esetében a két összeg közül a magasabb alkalmazandó. Az ellenőrzési és szankcionálási feladatokat az illetékes nemzeti hatóságok látják el. Az Európai Bizottság is rendelkezik ellenőrzési és bírságolási jogosultságokkal az általános célú MI-modellek szolgáltatóival szemben.

Külön hangsúlyozni kell, hogy a személyes adatok jogellenes kezelése miatt a Nemzeti Adatvédelmi és Információszabadság Hatóság (NAIH) is eljárhat. **Példa:** egy bank ügyfélszolgálati rendszerének ügyében a hangfelvételek automatikus elemzése és az érzelmi állapot vizsgálata miatt 250 millió forintos adatvédelmi bírságot szabtak ki.

Vezetői következtetések és javasolt vállalati intézkedések

A dokumentum alapján a mesterséges intelligencia vállalati alkalmazása nem pusztán informatikai vagy hatékonyságnövelési kérdés. Egyidejűleg jogi, adatvédelmi, információbiztonsági, munkajogi és üzletmenet-folytonossági kérdés is.

Egy vállalat számára az alábbi intézkedések indokoltak lehetnek:

Terület	Javasolt intézkedés
MI-használati szabályzat	A vállalati MI-használat írásos szabályozása
Engedélyezett rendszerek	A használható MI-eszközök és szolgáltatók meghatározása
Adatvédelem	Személyes adatok bevitelének szabályozása, GDPR-megfelelőség vizsgálata
Üzleti titok	Bizalmas dokumentumok, know-how és üzleti titok feltöltésének korlátozása
Szerzői jog	A bemeneti és generált tartalmak jogszerű felhasználásának ellenőrzése
MI-jártasság	Munkavállalói oktatás és tudatosságnövelés

Emberi ellenőrzés	Az MI által előállított eredmények szakmai validálása
Kockázatkezelés	Az alkalmazott MI-rendszerek kockázati besorolása és dokumentálása
Magas kockázatú alkalmazások	A különleges megfelelőségi és emberi felügyeleti követelmények teljesítése
Felelősség	A használati jogosultságok, ellenőrzési feladatok és felelősségi körök meghatározása

Javasolt gyakorlati bevezetési sorrend

1. **MI-rendszerek használatának felmérése és esetleg leltározása**
   Fel kell mérni, hogy a vállalat és a vállalat munkavállalói milyen MI-eszközöket használnak, milyen célra és milyen adatokkal. A nem vállalati licencek használatának korlátozása, tiltása.
2. **Kockázati besorolás**
   Meg kell határozni az egyes rendszerek AI Act szerinti kockázati kategóriáját és a kapcsolódó kötelezettségeket.
3. **Adatbiztonsági korlátozások**
   Meg kell határozni, hogy milyen adatokat lehet és milyeneket tilos külső MI-rendszerbe továbbítani.
4. **Belső szabályzat kialakítása**
   Rögzíteni kell az engedélyezett eszközöket, a használat célját, a felelősségi köröket és az ellenőrzési folyamatokat.
5. **Munkavállalói oktatás**
   Biztosítani kell a megfelelő MI-jártasságot és a biztonságos használathoz szükséges ismereteket.
6. **Ellenőrzés és folyamatos felülvizsgálat**
   Rendszeresen felül kell vizsgálni a használt MI-eszközöket, a szolgáltatói feltételeket és a vállalati gyakorlatot.

Összegző vezetői álláspont

A dokumentum legfontosabb üzenete, hogy a mesterséges intelligencia használatából eredő jogi-és üzleti kockázatok nem háríthatók át az MI-szolgáltatóra. A vállalatnak alkalmazóként is felelőssége van a rendszer megfelelő használatáért, az adatok védelméért és az MI által előállított eredmények ellenőrzéséért.

Különösen három terület kritikus:

1. **Információbiztonság:** A munkavállalók ne adhassanak át ellenőrizetlen külső MI-szolgáltatásoknak személyes adatokat, üzleti titkokat vagy más védett információkat.
2. **Felelősségi és ellenőrzési rendszer:** Az MI által előállított tartalom nem tekinthető automatikusan hitelesnek. A felhasználásért felelős személynek ellenőriznie kell annak helyességét.

3. **Szabályozott vállalati működés:** Szükséges az engedélyezett MI-rendszerek, a használati feltételek, a jogosultságok és a munkavállalói kötelezettségek írásos meghatározása.

Végső következtetés: Az MI vállalati használatát nem célszerű tiltással megakadályozni, de szabályozatlanul engedélyezni sem. A megfelelő megoldás egy dokumentált, kockázatalapú, ellenőrizhető és felelősségi körökhöz rendelt vállalati MI használati rendszer kialakítása.